

- [90] P. M. Phothilimthana, A. Thakur, R. Bodik, and D. Dhurjati, “Scaling up superoptimization,” *SIGARCH Comput. Archit. News*, vol. 44, p. 297–310, mar 2016.
- [91] T. Jackson, *On the Design, Implications, and Effects of Implementing Software Diversity for Security*. PhD thesis, University of California, Irvine, 2012.
- [92] R. El-Khalil and A. D. Keromytis, “Hydan: Hiding information in program binaries,” in *Information and Communications Security* (J. Lopez, S. Qing, and E. Okamoto, eds.), (Berlin, Heidelberg), pp. 187–199, Springer Berlin Heidelberg, 2004.
- [93] V. Singhal, A. A. Pillai, C. Saumya, M. Kulkarni, and A. Machiry, “Cornucopia: A framework for feedback guided generation of binaries,” in *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*, ASE ’22, (New York, NY, USA), Association for Computing Machinery, 2023.
- [94] B. Cox, D. Evans, A. Filipi, J. Rowanhill, W. Hu, J. Davidson, J. Knight, A. Nguyen-Tuong, and J. Hiser, “N-variant systems: a secretless framework for security through diversity,” in *Proc. of USENIX Security Symposium*, USENIX-SS’06, 2006.
- [95] D. Bruschi, L. Cavallaro, and A. Lanzi, “Diversified process replicas for defeating memory error exploits,” in *Proc. of the Int. Performance, Computing, and Communications Conference*, 2007.
- [96] B. Salamat, A. Gal, T. Jackson, K. Manivannan, G. Wagner, and M. Franz, “Stopping buffer overflow attacks at run-time: Simultaneous multi-variant program execution on a multicore processor,” tech. rep., Technical Report 07-13, School of Information and Computer Sciences, UC Irvine, 2007.
- [97] G. Agosta, A. Barengi, G. Pelosi, and M. Scandale, “The MEET approach: Securing cryptographic embedded software against side channel attacks,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 8, pp. 1320–1333, 2015.
- [98] T. Jackson, B. Salamat, A. Homescu, K. Manivannan, G. Wagner, A. Gal, S. Brunthaler, C. Wimmer, and M. Franz, “Compiler-generated software diversity,” in *Moving Target Defense*, pp. 77–98, Springer, 2011.
- [99] A. Amarilli, S. Müller, D. Naccache, D. Page, P. Rauzy, and M. Tunstall, “Can code polymorphism limit information leakage?,” in *IFIP International Workshop on Information Security Theory and Practices*, pp. 1–21, Springer, 2011.

- [100] A. Voulimeneas, D. Song, P. Larsen, M. Franz, and S. Volckaert, “dmvx: Secure and efficient multi-variant execution in a distributed setting,” in *Proceedings of the 14th European Workshop on Systems Security*, pp. 41–47, 2021.
- [101] C. Fred, “Computer viruses,” in *Proceedings of the 7th DoD/NBS Computer Security Conference 1984*, pp. 240–263, 1986.
- [102] R. L. Castro, C. Schmitt, and G. D. Rodosek, “Armed: How automatic malware modifications can evade static detection?,” in *2019 5th International Conference on Information Management (ICIM)*, pp. 20–27, 2019.
- [103] R. L. Castro, C. Schmitt, and G. Dreo, “Aimed: Evolving malware with genetic programming to evade detection,” in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 240–247, IEEE, 2019.
- [104] H. Aghakhani, F. Gritti, F. Mecca, M. Lindorfer, S. Ortolani, D. Balzarotti, G. Vigna, and C. Kruegel, “When malware is packin’ heat: limits of machine learning classifiers based on static analysis features,” in *Proc. of NDSS*, 2020.
- [105] M. Chua and V. Balachandran, “Effectiveness of android obfuscation on evading anti-malware,” in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, CODASPY ’18, Association for Computing Machinery, 2018.
- [106] P. Dasgupta and Z. Osman, “A Comparison of State-of-the-Art Techniques for Generating Adversarial Malware Binaries,” *arXiv e-prints*, Nov. 2021.
- [107] H. Bostani and V. Moonsamy, “Evadedroid: A practical evasion attack on machine learning for black-box android malware detection,” *CoRR*, vol. abs/2110.03301, 2021.
- [108] G. Lu and S. K. Debray, “Weaknesses in defenses against web-borne malware - (short paper),” in *Detection of Intrusions and Malware, and Vulnerability Assessment - 10th International Conference, DIMVA. Proceedings* (K. Rieck, P. Stewin, and J. Seifert, eds.), Lecture Notes in Computer Science, 2013.
- [109] M. Payer, “Embracing the new threat: Towards automatically self-diversifying malware,”
- [110] N. Loose, F. Mächtle, C. Pott, V. Bezsmertnyi, and T. Eisenbarth, “Madvex: Instrumentation-based Adversarial Attacks on Machine Learning Malware Detection,” *arXiv e-prints*, p. arXiv:2305.02559, May 2023.
- [111] J. Cabrera Arteaga, O. Floros, O. Vera Perez, B. Baudry, and M. Monperrus, “Crow: code diversification for webassembly,” in *MADWeb, NDSS 2021*, 2021.